FACTSHEET: KENYA

Last updated: 31 March 2020
Prepared by Tshepiso Hadebe

FAST FACTS

Population: 51,393,010
Capital: Nairobi
President: Uhuru Kenyatta
2019 Freedom House Score: 48/100
Data protection law? Yes

LAW

The Data Protection Act No. 24 of 2019 (the Act) was signed into law in November 2019 and sets out the regulatory framework for data protection in Kenya. It sets out guidelines on how personally identifiable data can be used, stored or shared.

Among other things, data subjects have the right to:

- be informed of the use to which their personal data is to be put;
- access to their personal data in custody of the data controller or data processor;
- object to the processing of all or part of their personal data;
- the correction of false or misleading data; and
- the deletion of false or misleading data.

PERSONAL DATA

Under the Act, personal data means any information relating to an identified or identifiable natural person. Sensitive personal data means any data revealing the natural person's:

- health status;
- ethnic social origin;
- conscience;
- belief;
- genetic data;
- biometric data;
- property details;
- marital status; and
- family details including names of a person's children, parents, spouse, sex or sexual orientation of the data subject.

COLLECTION AND PROCESSING

A data controller or data processor shall collect personal data directly from the data subject. Personal data maybe collected indirectly where—

- the data is contained in a public record;
- the data subject has deliberately made the data public;
- the data subject has consented to collection from another source;
- the data subject has an incapacity, the guardian appointed has consented to the collection from another source;
- the collection from another source would not prejudice the interests of the data subject;
- collection of data from another source is necessary—
    - for the prevention, detection, investigation, prosecution and punishment of a crime;
    - for the enforcement of a law which imposes a pecuniary penalty; or
    - for the protection of the interests of the data subject or another person.

A data controller or data processor shall collect, store or use personal data for purposes which are lawful, specific and explicitly defined.

Every data controller or data processor shall ensure that personal data is:

- processed in accordance with the right to privacy of the data subject;
- processed lawfully, fairly and in a transparent manner in relation to any data subject;
- collected for the explicit, specified and legitimate purposes and not further processed in a manner incompatible with those purposes;
- adequate, relevant, limited to what is necessary in relation to the purpose for which it is processed;
- collected only where a valid explanation is provided whenever information relating to family or private affairs is required;
- accurate and, where necessary, kept up to date, with every reasonable step being taken to ensure that any inaccurate personal data is erased or rectified without delay;
- kept in form which identifies the data subjects for no longer than is necessary for the purposes which it was collected; and
- not transferred outside of Kenya, unless there is proof of adequate data protection safeguards or consent from the data subject.

REGISTRATION AND ENFORCEMENT

The Act establishes the office of the Data Protection Commissioner (Commissioner). The Commissioner has enforcement powers and may investigate complains about regulatory violations, but as it stands the Commissioner has not yet been appointed.

The Act states that no person shall act as a data controller or data processor unless registered with the Commissioner. Where a data controller or data processor meets the requirements for registration, the Commissioner will issue a certificate of registration. Each data controller may also appoint a data protection officer who is responsible for compliance issues related to data collection or processing.

Where the Commissioner is satisfied that a person has failed or is failing to comply with any provision of the Act, the Commissioner may serve an enforcement notice on that person requiring that person to take such steps within such period as may be specified in the notice. Any person who, without reasonable excuse, fails to comply with an enforcement notice commits an offence and is liable on conviction to a fine not exceeding five million shillings or to imprisonment for a term not exceeding two years, or to both.

CROSS-BORDER TRANSFER

A data controller or data processor may transfer personal data to another country only where:

- the data controller or processor has given proof to the Data Commissioner on the appropriate safeguards with respect to the security and protection of personal data;
- the data controller or processor has given proof to the Data Commissioner of the appropriate safeguards with respect to the security and the protection of personal data, and the appropriate safeguards including jurisdictions with corresponding data protection laws;
- the transfer is necessary—
    - for the performance of a contract between the data subject and the data controller or data processor or implementation of pre-contractual measures taken at the data subject's request;
    - for the conclusion or performance of a contract concluded in the interest of the data subject between the controller and another person;
    - for any matter of public interest;
    - for the establishment, exercise or defence of a legal claim;
    - to protect the vital interest of the data subject or of other persons, where the data subject is physically or legally incapable of giving consent; or
    - for compelling legitimate interests pursued by the data controller or data processor, which are not overridden by the interests, rights and freedoms of data subjects.

SECURITY AND BREACH PROTOCOL

In case of a personal data breach where there is a real risk of harm to the data subject whose data has been breached, a data controller must notify the Commissioner without delay within 72 hours of becoming aware of the breach. They must also communicate to the data subject in writing within a reasonably practical period, unless the identity of the data subject cannot be established. In cases where the data processor becomes aware of a personal data breach, they must notify the data controller within 48 hours.

The communication of the breach to the data subject shall not be required where the data controller or data processor has implemented appropriate security safeguards which may include encryption of affected personal data.

Read the legal notice and terms of use for this factsheet.